

Forum:[Hack Forums](#)

Thread: [\[FREE\] DNS Nativeness Checker -> How anti-fraud systems see your proxies](#)

ZloyTeam - September 15, 2026, 1:45 pm

Greetings, community.

Companies detect Proxies and VPNs by just two basic parameters — IP and DNS. And while everyone has already learned to check the former against blacklists, DNS settings still remain a complete mystery to many.

The reality is that anti-fraud systems (Cloudflare, Stripe, Amazon...) know perfectly well what DNS resolvers, EDNS Client Subnet (ECS), and various latencies should look like for a legitimate user. But for some reason, sellers do not always pay due attention to proper DNS configuration. We regularly see situations where a client is sold an expensive US IP, but their resolvers route through Indonesia (and this happens even with top providers).

There was a time when checking IPs for cleanliness became standard practice. It is time to push for a new standard — DNS checking.

The Zloy.Team presents a FREE tool for deep analysis of DNS fingerprints.

? ZLOY DETECT | DNS Nativeness Checker:

<https://dnsdetect.zl0y.team/>

How it works:

Previously, such solutions were available only to large enterprises. After half a year of research based on >30 million real fingerprints, we have created a dynamically evolving correlation matrix.

The algorithm analyzes 170 parameters, runs them through >2.5 million rules, and answers a single question: does your DNS match the average clean fingerprint in the US?

The system outputs a mathematical probability:

Clean (real native user)

VPN (including server gateways)

Proxy

What to do with this:

Go to the site and check your daily consumables. If the DNS is subpar and the scoring confidently points to "Proxy" - it's up to you to decide whether to continue working with such a Proxy or not.

Spoiler: If you see the coveted "Clean" - don't flatter yourself. Your DNS settings might be fine, but our internal anti-fraud system is still capable of recognizing the use of an anti-detect browser or a virtual machine. In the future, we will roll out a global update on the main zl0y.team project, and there we will scare you even more. And the "magic pill" for all these problems is already being prepared for integration into our [ZloyRouter](#) hardware gateway.

We look forward to constructive feedback in this thread.

P.S. For proxy providers, we have an API so that your clients can understand what Proxies they are buying BEFORE they pay — reach out to us.

P.P.S. The tool is free, no registration required, and we continue to develop and improve it – everything for the market, everything for the people.

ZloyTeam - *October 12, 2026, 3:27 am*

For those who have already tested the checker and are wondering how accurate and detailed the mathematical model is — we've prepared an article with an under-the-microscope breakdown.

In it, we ran popular proxies from 9Proxy and Nsocks through our service and analyzed the triggers of anti-fraud systems using real-world examples:

Why a perfect residential IP gets flagged due to stripped WebRTC;

How "dirty" DNS resolvers give you away (and why manual ECS spoofing won't save you);

A hands-on test of expensive proxies (\$1/piece) that the algorithm identifies as 91% Proxy.

? Read the article with the full breakdown and tests:

https://blog.zl0y.team/blog/dns_nativeness_checker

If anyone testing the service has encountered similar anomalies (where the IP is clean, but the scoring still flags it as a Proxy) — drop your results, and we'll discuss why this happens.